

Texas DIR OCISO Overview



Texas Department of Information Resources

Transforming How
Texas Government
Serves Texans

Introductions

Jeremy Wilson

Deputy CISO, Security Operations/CIRT



Office of the Chief Information Security Officer
Texas Department of Information Resources



DIR Overview

Mission

To serve Texas government by:

- Leading the state's technology strategy,
- Protecting state technology infrastructure, and
- Offering innovative and cost-effective solutions for all levels of government.

Vision

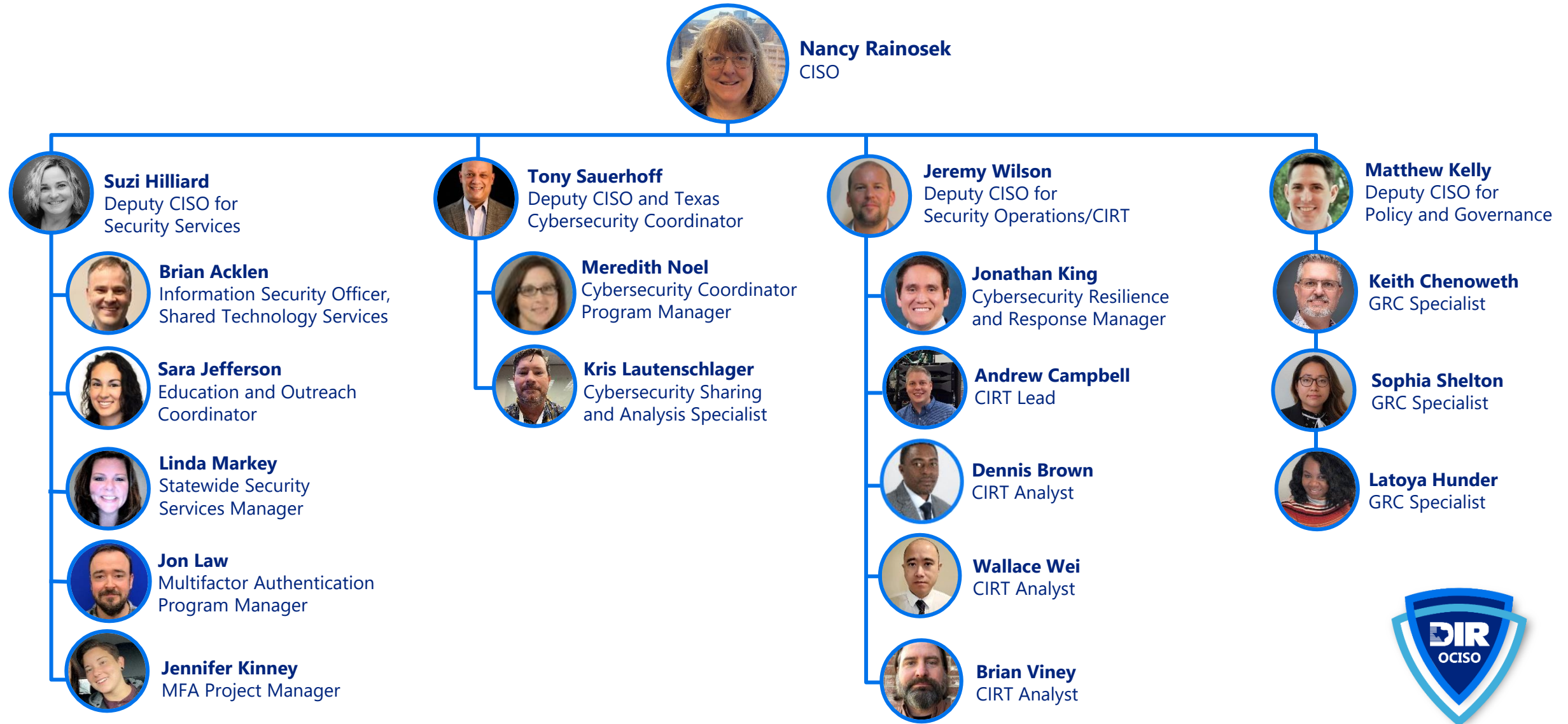
Transforming How Texas Government Serves Texans





Office of the Chief Information Security Officer (OCISO)

Meet the Team

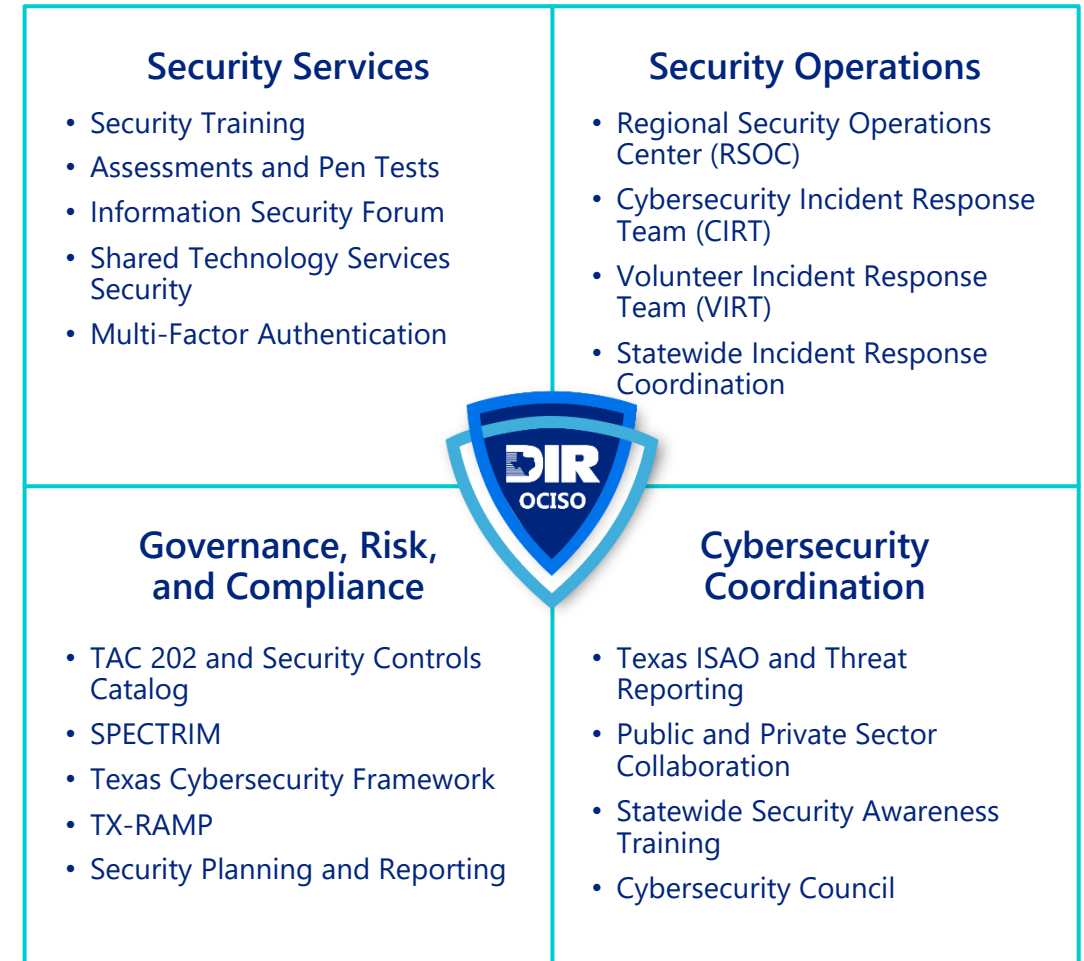



OCISO Program Areas and Functions

OCISO's Approach

Working to make Texas more secure through:

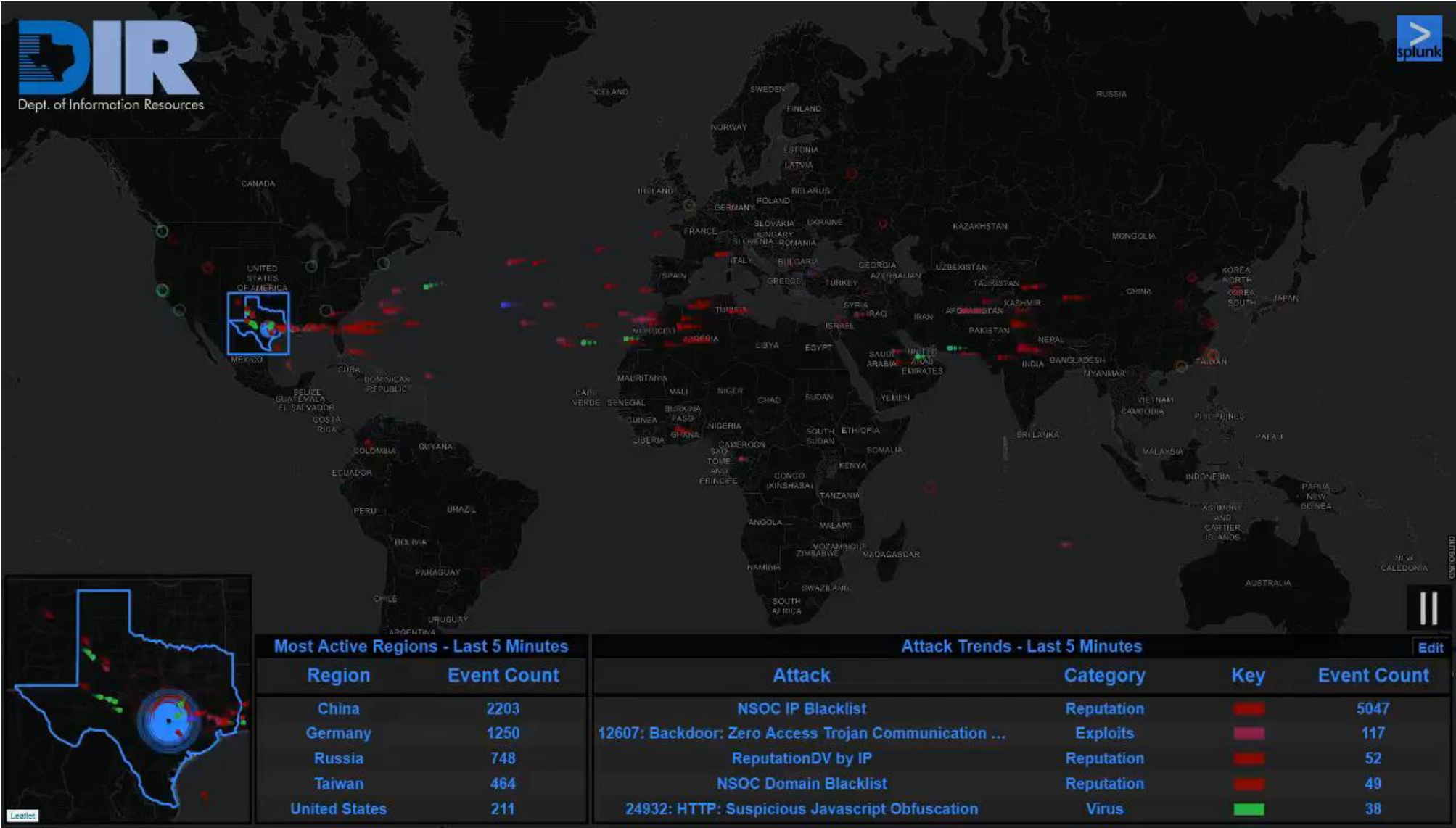
- Community Engagement,
- Information Sharing, and
- Strengthening the States' Security Posture





Regional Security Operations Centers (RSOCs)

TX Heat Map/Big Data Visualization Project



Regional Security Operations Center (RSOC) Pilot Award

Senate Bill 475

- This solution envisions starting with one regional Security Operations Center (SOC), and eventually expanding to multiple SOC's located at universities in the geographically dispersed Comptroller of Public Accounts twelve economic regions across Texas.
- This will allow for "boots on the ground" close to local governments that may need assistance with major cybersecurity incidents in each region.
- It also contemplates the use of student workers, thereby offsetting staffing costs and simultaneously providing real-world training for the much-needed cybersecurity professionals of the future.
- RSOC pilot awarded to Angelo State University



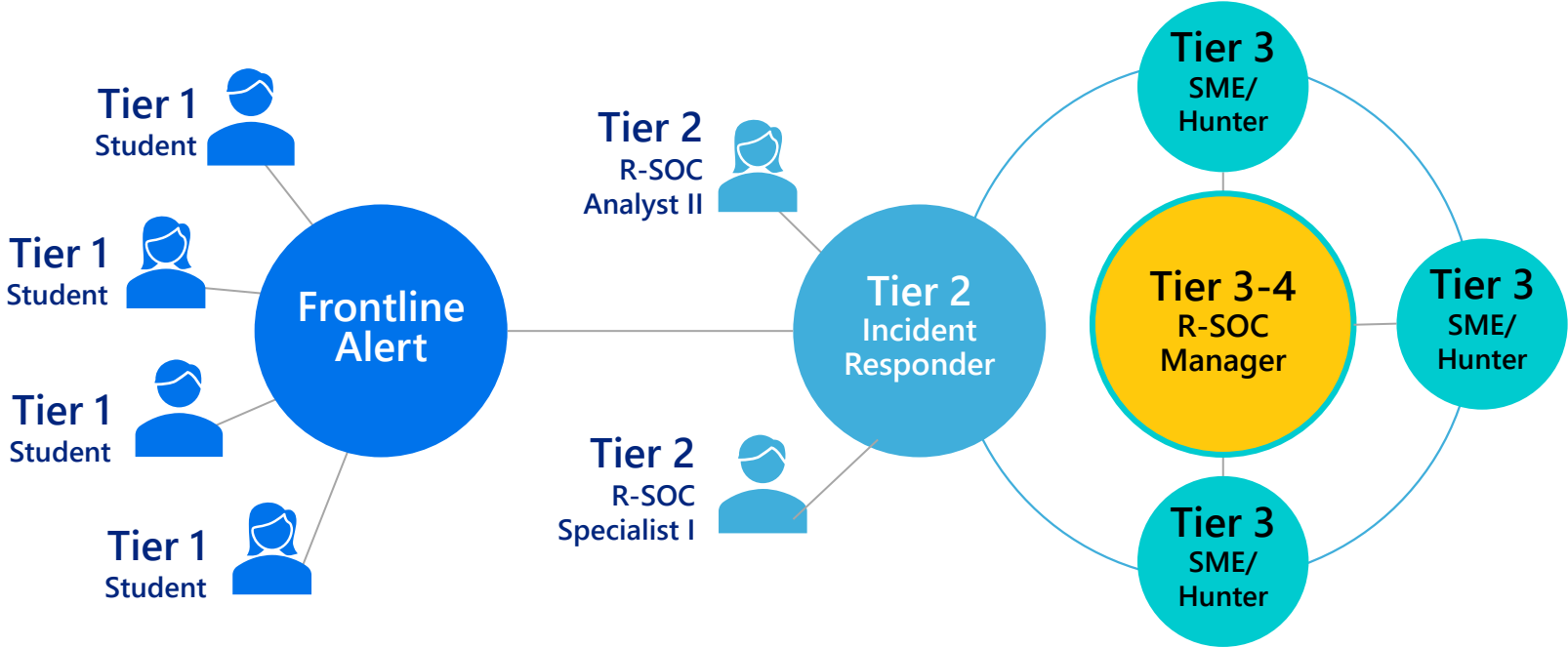
SB 475: Regional Network Security Centers Services

1. **Real-time network security monitoring** to detect and respond to network security events that may jeopardize this state and the residents of this state
2. **Alerts and guidance** for defeating network security threats, including firewall configuration, installation, management, and monitoring, intelligence gathering, and protocol analysis;
3. **Immediate response** to counter network security activity that exposes this state and the residents of this state to risk, including complete intrusion detection system installation, management, and monitoring for participating entities;
4. **Development, coordination, and execution of statewide cybersecurity operations** to isolate, contain, and mitigate the impact of network security incidents for participating entities;
5. **Cybersecurity educational services**



R-SOC Reporting Chart

Pre-Phase Activities Expression of Interest		Phase 1 Establish R-SOC and Pilot						Phase 2 Run and Enhance R-SOC	
		2022						2023	
February - July		July	August	September	October	November	December	January – March	April – August



Tier 1	Tier 2	Tier 3	Tier 4
First line incident responder; alerts and urgency.	Follow procedures to remediate problem; flag issues for further investigation.	High level security analysts; use advanced threat detection tools; make recommendations on security.	R-SOC Manager/Director; oversee teams; hires and trains, evaluates performance; compliance.

R-SOC Room Visualization @ ASU



The background is a dark blue field filled with a network of white lines and circular nodes. Various white line-art icons are scattered throughout, representing different aspects of cybersecurity: a warning triangle, an eye, a hand pointing at a keypad, a USB drive, a credit card, a safe, a key, a document with a shield, a Wi-Fi signal, a magnifying glass, an envelope, and a server rack. The overall theme is digital security and incident response.

Cybersecurity Incident Response Team (CIRT)

Security Operations/ CIRT Overview and Staffing

Security Operations/ CIRT Program Areas

- Cybersecurity Incident Response Team (CIRT)
- Statewide Incident Response Coordination
- Regional Security Operations Center (RSOC)
- Volunteer Incident Response Team (VIRT)

CIRT Mission Statement

The Texas DIR Cybersecurity Incident Response Team (CIRT) provides incident response support to eligible organizations to safeguard the state's critical assets.

CIRT Hiring Update

- Upcoming positions



CIRT Update – Preparation Activities

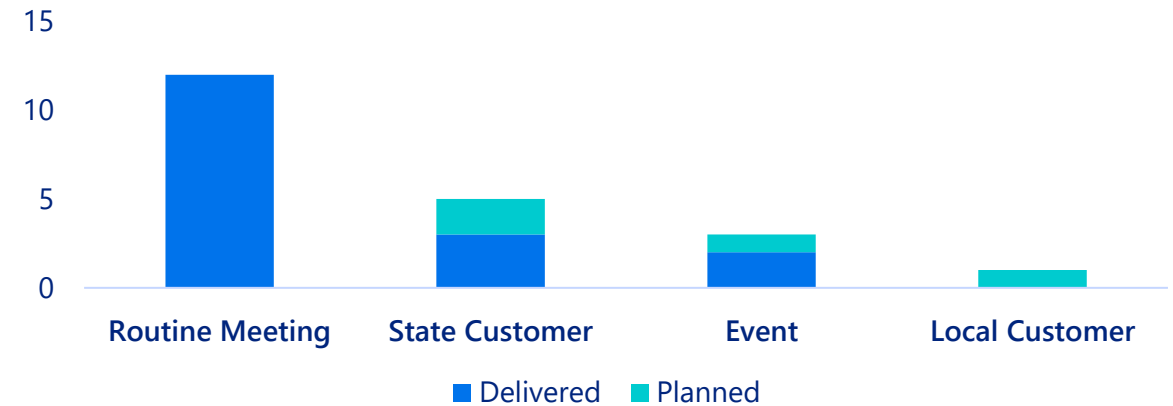
Tabletop Exercise Deliveries

- Custom tabletops developed and delivered to eligible customers
- TX-ISAO and Monthly Security meetings
- Events such as TAGITM and 2022 ISF
- State agencies and local governments
- Participation with ASU RSOC and additional partners

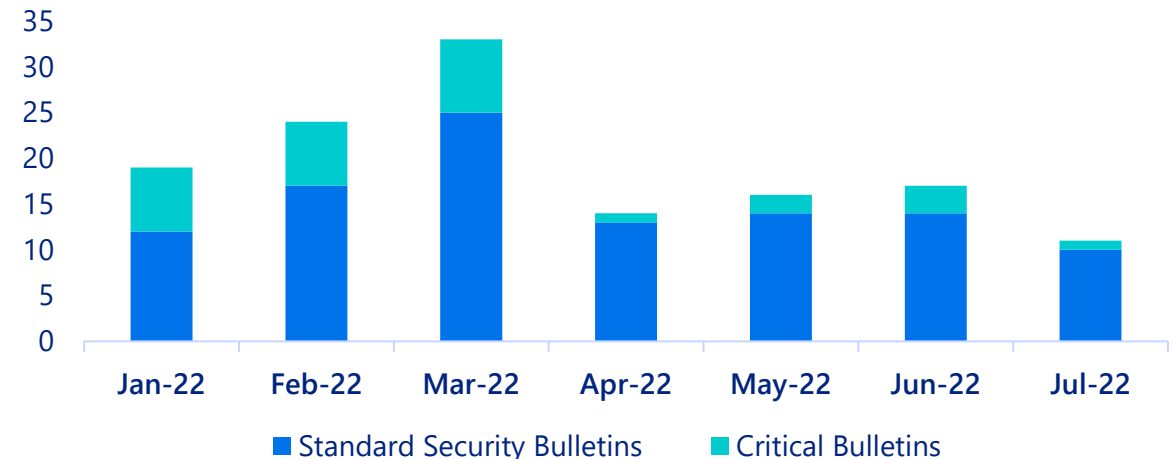
TX-ISAO Security Bulletin Distribution

- Focus on combining bulletins
- Provide actionable intelligence, first
- Spike in bulletins attributed to geopolitical tensions
- Added weekly DIR CyOps Threat Intelligence bulletin

Year to Date – Tabletop Exercise Deliveries



Year to Date - Security Bulletin Distribution



CIRT Update – Operational Activities

CIRT Event Tracker

Planning and Documentation

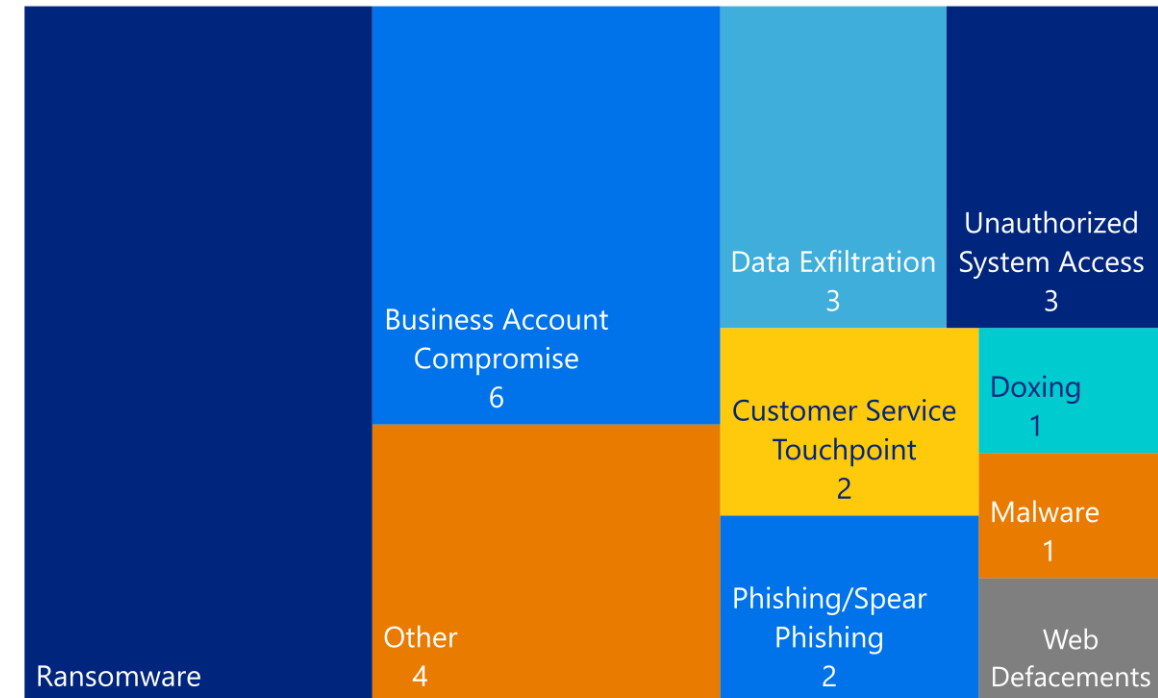
- DIR Incident Response Plan revision
- Incident Response Team Redbook revision
- CIRT Playbook development
- CIRT Procedures and Equipment outfit
- Homeland Security Strategic Plan Metrics
- Security Bulletin Distribution Guide development

Incident Response Workgroup Expansion

CIRT Staff Onboarding and Training

Regional Security Operation Center Pilot

Year to Date - CIRT Events Tracker



CIRT Update – Incident Impacts and Observations

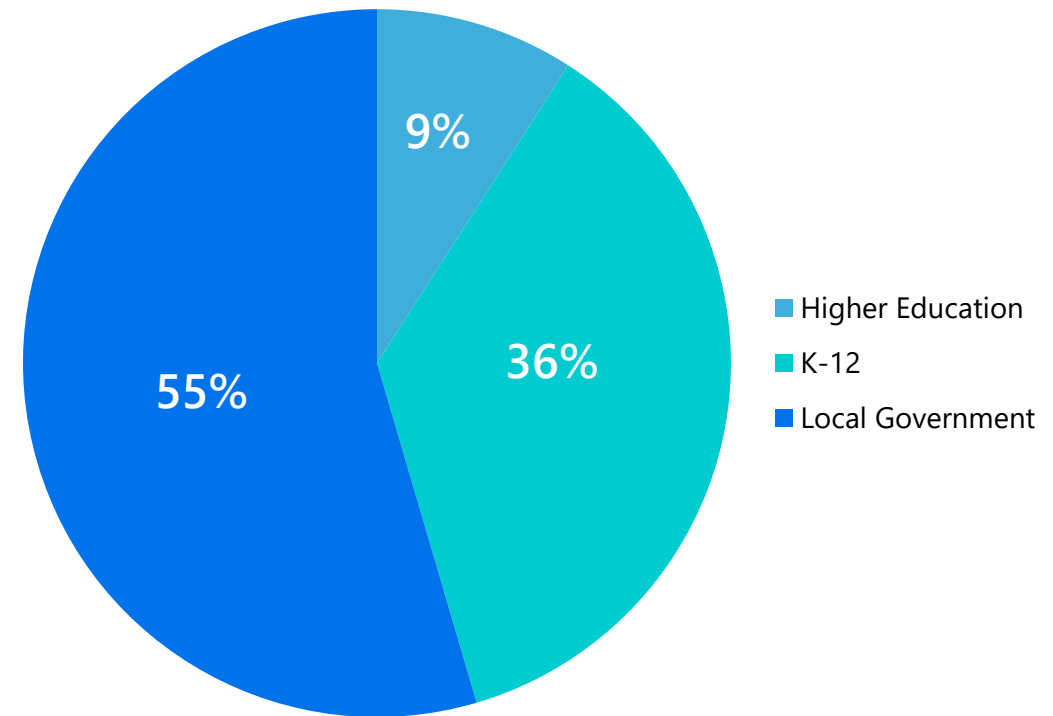
Ransomware Activity Trends

- End of life equipment, unpatched vulnerabilities exploited, and credential access exploited
- Propagation via unauthorized remote access tools
- Unsecured data backups specifically targeted by threat actors
- Data exfiltration and secondary impacts continue
- EDR, monitoring, and secure backups significantly limited impacts for several organizations

CIRT Incident Support Activities

- **June 2022: First DIR CIRT deployment to support impacted entity with IR activities**
- Continued remote guidance, resource coordination, technical assistance, and reporting

Year to Date - Texas Entities Impacted by Ransomware Reported to DIR





Volunteer Incident Response Team(VIRT)

Texas VIRT Overview

Purpose

- The Texas Volunteer Incident Response Team (VIRT) provides eligible public entities rapid cybersecurity incident response assistance

Deployment

- Major statewide cybersecurity disaster with a Governor issues cyber disaster declaration
- When multiple entities are affected

Logistics

- Deployed and coordinated by DIR
- Travel reimbursements provided for state assigned missions
- Training opportunities available for volunteers

Benefits

- Assist government organization in Texas respond to a major cybersecurity incident



Texas VIRT Overview

Application Process

- Review program handbook and apply for membership
- Received applications review by DIR OCISO
- Volunteer background check
- Sign volunteer contract (NDA)

Qualifications

- Cybersecurity IR experience preferred
- Information Technology and Project Management encouraged to apply

Resources

- [VIRT Homepage](#)
- [Texas VIRT Program Handbook](#)
- [VIRT Volunteer Application Form](#)
- Questions? TexasVIRT@dir.texas.gov





Requesting Incident Response Assistance


Requesting Incident Response Assistance

Calling Texas DIR for Assistance

- Place call to 1-877-347-2476
- Provide an overview of situation and request incident response assistance

DIR Cyber Incident Response Assistance

- Discussions and guidance
- Connection to insurance provider
- Onsite or remote DIR CIRT support
- Managed Security Services support
- Connection to state and federal law enforcement

**Office of the Chief
Information Security Officer**

**Cybersecurity
Resources**

Basic Cyber Hygiene

- Manage your IT and risk.
- Know your systems, where your data is, and who has access.
- Harden your systems – CIS benchmark (<https://www.cisecurity.org/cis-benchmarks/>) is one way.
- Keep your systems updated – patch, keep your anti-virus up to date, and use vendor supported versions.
- Monitor your systems for strange behavior.
- Applications – Open Web Application Security Project (OWASP) and public scan with a tool such as SSL Labs (<https://www.ssllabs.com/ssltest/>).

Adopt a Framework

There are many that exist. Texas state agencies use the Texas Cybersecurity Framework (<https://bit.ly/2Ni4Pod>) or choose another that works better for you such as NIST CSF, CMMI, and CCSMM.

Get a Cybersecurity assessment

An assessment will let you know how you are doing and can be the basis for modernization, investment, and planning.

There are numerous sources that offer assessments and can even be done at no cost. DIR, the Department of Homeland Security (DHS), or various third parties provide assessments as well.

Have an Incident Response Plan

There are many sample plans on the Internet. The plan should be used in conjunction with Business Continuity planning. DIR offers a template as well: <https://bit.ly/32hjUe8>

Join MS-ISAC

- The DHS Multi-State Information Sharing and Analysis Center (MS-ISAC) offers many services.
- Learn more from this free resource: <https://learn.cisecurity.org/ms-isac-registration>
- Complete the Nationwide Cybersecurity Review (NCSR) to identify areas to improve.

Join the Texas ISAO

The Texas ISAO (isao.texas.gov) provides a mechanism for state and non-state entities in Texas to share actionable and timely information regarding cybersecurity threats, best practices, and remediation strategies.

CISA/DHS Services and resources

- <https://www.us-cert.gov/resources/ncats>
- <https://www.cisa.gov/cyber-essentials>

DIR Resources

- DIR Security Services: <https://bit.ly/31Ta6uf>
- Managed Security Services: <https://bit.ly/2Ni1GUU>
- Complete a Managed Security Services (MSS) Contract through DIR. This is a no-cost option that keeps MSS on retainer and at the ready if needed.


Fraud Resource

- Cybercrime Support Network: <https://fraudsupport.org/>
- Data Breach and Credit Monitoring Services: <http://www.txsmartbuy.com/contracts/view/2192>

Train

- <https://www.preparingtexas.org/TrainingCatalog.aspx> (keyword "Cyber")
- <https://cyberready.org/training/>
- Federal Virtual Training Environment (free for SLTT): <https://fedvte.usalearning.gov>

Work with your designated emergency management personnel to optimize resources and minimize the impact of an incident.

**If You Need Assistance**

Contact your Emergency Management Coordinator or Texas Division of Emergency Management (TDEM) District Coordinator <https://tdem.texas.gov/field-response/>. Or, contact DIR Office of the CISO at 1-877-DIR-CISO (1-877-347-2476) or by email at DIRSecurity@dir.texas.gov.

Texas Department of Information Resources | dir.texas.gov | #DIRisIT | @TexasDIR

Building and Sustaining an Effective Security Program

Cybersecurity as a Priority

- Texas DIR
- State legislature
- Federal government

People

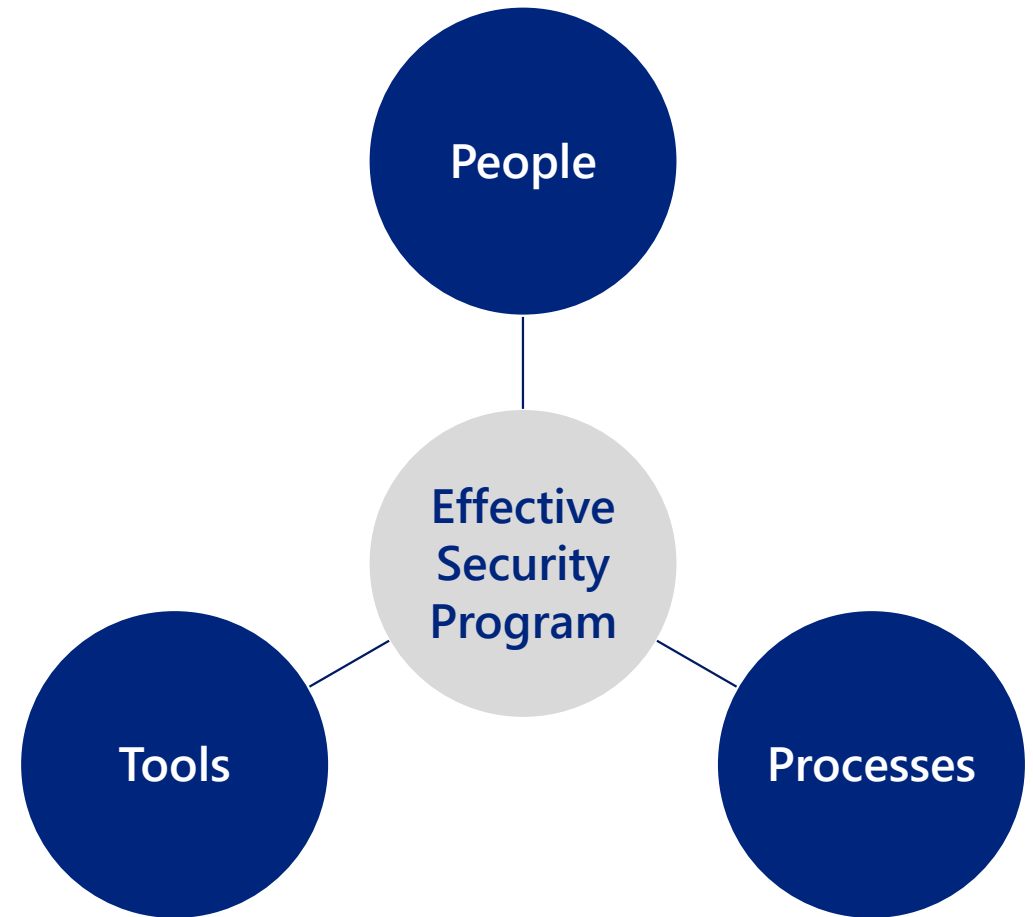
- Empower your security professionals.
- Conduct realistic training and exercises for the entire organization.

Processes

- Develop clear policies and procedures.
- Update and socialize documentation.

Tools

- Conduct a proof of concept for new equipment.
- Ensure tools are effective and support your security program.





Supporting Resources

Informational Resources

Guides

- DIR [Incident Response Team Redbook](#)
- MS-ISAC/CISA [Joint Ransomware Guide](#)
- MS-ISAC [First Steps Within a Cybersecurity Program](#)
- American Public Power Association [Public Power Cyber Incident Response Playbook](#)

Training

- Federal Virtual Training Environment (FedVTE) [Free Online Cybersecurity Training](#)
- Texas DIR [Statewide Cybersecurity Awareness Training Resources](#)

Membership

- Texas ISAO [TxISAO Mailing List Access Request Form](#)
- MS-ISAC [Join MS-ISAC](#)
- InfraGard [New Application](#)



Response Resources

ISAO Contact Information

- Website: <https://dir.texas.gov/information-security/txisao>
- Mailing list sign up and threat reporting form
- Email: ISAO@dir.texas.gov

DIR Cyber Operations (NSOC)

- Email for phishing email reporting: security-alerts@dir.texas.gov

DIR Cyber Incident Response Support

- 24x7x365 incident response and assistance hotline for state and local government organizations: [1-877-DIR-CISO](tel:1-877-DIR-CISO) ([1-877-347-2476](tel:1-877-347-2476))

Incident Response Resources

- DIR [Managed Security Services](#)
- Texas base cyber insurance risk pools:
 - [Texas Association of Counties \(TAC\)](#)
 - [Texas Municipal League \(TML\)](#)
 - [Texas Association of School Boards \(TASB\)](#)



Thank You!

dir.texas.gov

#DIRisIT

@TexasDIR



Texas Department of Information Resources

Transforming How
Texas Government
Serves Texans